

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of)
SATO et al.)
Application Number: To be Assigned)
Filed: Concurrently Herewith)
For: BANK SYSTEM PROGRAM, CREDIT)
SERVICE PROGRAM AND IC CARD)
ATTORNEY DOCKET NO. NITT.0168)

Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231

**REQUEST FOR PRIORITY
UNDER 35 U.S.C. § 119
AND THE INTERNATIONAL CONVENTION**

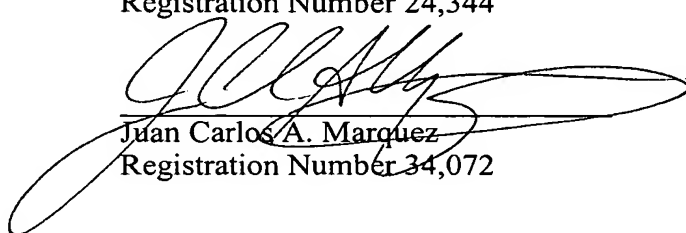
Sir:

In the matter of the above-captioned application for a United States patent, notice is hereby given that the Applicant claims the priority date of December 20, 2002, the filing date of the corresponding Japanese patent application 2002-369174.

A certified copy of Japanese patent application 2002-369174 is being submitted herewith. Acknowledgment of receipt of the certified copy is respectfully requested in due course.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344



Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200
December 16, 2003

PATENT OFFICE

JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application : December 20, 2002
Application Number : Patent Application No. 2002-369174
Applicant (s) : Hitachi, Ltd.

Dated this 28th day of November, 2003

Yasuo IMAI
Commissioner,
Patent Office

Certificate No. 2003-3098608

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 2 月 2 0 日
Date of Application:

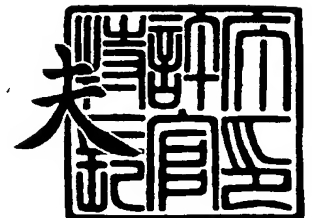
出 願 番 号 特 願 2 0 0 2 - 3 6 9 1 7 4
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 6 9 1 7 4]

出 願 人 株式会社日立製作所
Applicant(s):

2 0 0 3 年 1 1 月 2 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



出証番号 出証特 2 0 0 3 - 3 0 9 8 6 0 8

【書類名】 特許願

【整理番号】 H02015391A

【あて先】 特許庁長官 殿

【国際特許分類】 G06K 19/00

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

 【氏名】 佐藤 暁子

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

 【氏名】 三科 雄介

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社 日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

 【電話番号】 03-3212-1111

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ICカードを利用した決済システム

【特許請求の範囲】

【請求項 1】

ICカードを利用した、クレジットサービスの決済システムにおいて、
前記クレジットサービスの提供管理システムと、クレジット利用代金が引き落とされる銀行サービスの提供管理システムが独立して設けられ、
銀行サービス提供管理システムは、代金の振込み及び口座管理を行う銀行サービス提供管理処理部と、利用者ごとの個人口座と、利用者がクレジット代金を引き落とし日まで入金しておく共通の口座と、各銀行支店に設置されているATM端末を有し、
前記銀行サービス提供管理処理部が、予め契約を締結したクレジットサービス提供管理システムと公開鍵を交換する手段と、
利用者からのクレジット利用代金の入金を、前記共通の口座に入金し、入金したことを示すデータに署名暗号化処理を行った上で、利用者の所有するICカードに格納する手段と、
引き落とし日に、前記共通の口座あるいは利用者の個人口座からクレジット利用代金を引き出し、クレジットサービス提供管理システムへ振込む手段を有し、
クレジットサービス提供管理システムは、クレジット利用時の与信確認やクレジット利用者情報を管理するクレジットサービス提供管理処理部と、利用者ごとの与信情報を格納する与信情報データベースと、各加盟店でクレジット決済を行う暮れ時とサービス加盟店端末を有し、
前記クレジットサービス提供管理処理部が、予め契約を締結した銀行サービス提供管理システムと公開鍵を交換する手段と、
利用者がクレジット利用を要求した際に、利用者の与信情報を確認する手段と、
銀行サービスシステムがICカードに格納した、入金したことを示すデータを抽出し正当性を確認し、与信情報データベースに仮反映させる手段と、
引き落とし日に、銀行サービス提供管理システムからの振込みを受け付け、与信情報データベースに仮反映されている情報を確認する手段を有することを特徴と

するクレジットサービスの決済システム。

【請求項 2】

前記クレジットサービスの決済システムにおいて、

予め銀行サービス提供管理システムとクレジットサービス提供管理システム間で、お互いの公開鍵証明書を交換し、

銀行サービス提供管理システムが前記入金したことを示すデータを、クレジットサービス提供管理システムの公開鍵で暗号化処理を行い、自身の公開鍵で署名付与処理を行う手段を有し、

ICカードへ当該データを格納する際に、ICカード内の自身の所有する銀行サービスアプリケーションと通信を行い格納する手段を有し、

ICカードが、前記銀行サービスアプリケーションが受信したデータを、同じくICカード内に存在するクレジットサービスアプリケーションに転送あるいは、共有化する手段を有し、

クレジットサービス提供管理システムが、前記入金したことを示すデータを抽出する際は、ICカード内のクレジットサービスアプリケーションと通信を行い抽出する手段を有することを特徴とする、

請求項 1 記載のクレジットサービスの決済システム。

【請求項 3】

前記クレジットサービスの決済システムにおいて、

予め銀行サービス提供管理システムとクレジットサービス提供管理システム間で、お互いの公開鍵証明書を交換し、

予めクレジットサービス提供管理システムは銀行サービス提供管理システムにICカード内のクレジットサービスアプリケーションの公開鍵を渡しておき、

銀行サービス提供管理システムが前記入金したことを示すデータを、クレジットサービス提供管理システムの公開鍵で暗号化処理を行い、自身の公開鍵で署名付与処理を行う手段を有し、

ICカードへ当該データを格納する際に、前記クレジットサービス提供管理システムから受け取ったICカード内クレジットサービスアプリケーションの公開鍵を用いて、ICカード内のクレジットサービスアプリケーションと通信を行い格納する

手段を有し、

クレジットサービス提供管理システムが、前記入金したことを示すデータを抽出する際は、ICカード内のクレジットサービスアプリケーションと通信を行い抽出する手段を有することを特徴とする、

請求項 1 記載のクレジットサービスの決済システム。

【請求項 4】

ICカードを利用した、銀行サービスの提供管理システムにおいて、

銀行サービス提供管理システムは、代金の振込み及び口座管理を行う銀行サービス提供管理処理部と、利用者ごとの個人口座と、利用者がクレジット代金を引き落とし日まで入金しておく共通の口座と、各銀行支店に設置されているATM端末を有し、

前記銀行サービス提供管理処理部が、予め契約を締結したクレジットサービス提供管理システムと公開鍵を交換する手段と、

利用者からのクレジット利用代金の入金を、前記共通の口座に入金し、入金したことを示すデータに署名暗号化処理を行った上で、利用者の所有するICカードに格納する手段と、

引き落とし日に、前記共通の口座あるいは利用者の個人口座からクレジット利用代金を引き出し、クレジットサービス提供管理システムへ振込む手段を有することを特徴とする、

銀行サービス提供管理システム。

【請求項 5】

前記銀行サービス提供管理システムにおいて、

予めクレジットサービス提供管理システムとの間で、お互いの公開鍵証明書を交換し、

前記入金したことを示すデータを、クレジットサービス提供管理システムの公開鍵で暗号化処理を行い、自身の公開鍵で署名付与処理を行う手段を有し、

ICカードへ当該データを格納する際に、ICカード内の自身の所有する銀行サービスアプリケーションと通信を行い格納する手段を有することを特徴とする、

請求項 4 記載の銀行サービス提供管理システム。

【請求項 6】

前記銀行サービス提供管理システムにおいて、
予めクレジットサービス提供管理システム間で、お互いの公開鍵証明書を交換し、
予めクレジットサービス提供管理システムからICカード内のクレジットサービスアプリケーションの公開鍵を受け取り、
前記入金したことを示すデータを、クレジットサービス提供管理システムの公開鍵で暗号化処理を行い、自身の公開鍵で署名付与処理を行う手段を有し、
ICカードへ当該データを格納する際に、前記クレジットサービス提供管理システムから受け取ったICカード内クレジットサービスアプリケーションの公開鍵を用いて、ICカード内のクレジットサービスアプリケーションと通信を行い格納する手段を有し、
請求項 4 記載の銀行サービス提供管理システム。

【請求項 7】

ICカードを利用した、クレジットサービス提供管理システムにおいて、
クレジットサービス提供管理システムは、クレジット利用時の与信確認やクレジット利用者情報を管理するクレジットサービス提供管理処理部と、利用者ごとの与信情報を格納する与信情報データベースと、各加盟店でクレジット決済を行う暮れ時とサービス加盟店端末を有し、
予め契約を締結した銀行サービス提供管理システムと公開鍵を交換する手段と、
利用者がクレジット利用を要求した際に、利用者の与信情報を確認する手段と、
銀行サービスシステムがICカードに格納した、入金したことを示すデータを抽出し正当性を確認し、与信情報データベースに仮反映させる手段と、
引き落とし日に、銀行サービス提供管理システムからの振込みを受け付け、与信情報データベースに仮反映されている情報を確認する手段を有することを特徴とするクレジットサービス提供管理システム。

【請求項 8】

前記クレジットサービス提供管理システムにおいて、
予め銀行サービス提供管理システムとの間で、お互いの公開鍵証明書を交換し、

前記入金したことを示すデータを抽出する際は、ICカード内のクレジットサービスアプリケーションと通信を行い抽出する手段を有することを特徴とする、請求項7記載のクレジットサービス提供管理システム。

【請求項9】

前記クレジットサービス提供管理システムにおいて、
予め銀行サービス提供管理システムとの間で、お互いの公開鍵証明書を交換し、
予め銀行サービス提供管理システムにICカード内のクレジットサービスアプリケーションの公開鍵を渡しておき、
前記入金したことを示すデータを抽出する際は、ICカード内のクレジットサービスアプリケーションと通信を行い抽出する手段を有することを特徴とする、
請求項7記載のクレジットサービスの決済システム。

【請求項10】

請求項1から9の何れか1つに記載のシステムにおいて、
入金したことを示すデータに、利用者氏名、利用者ID、入金額、入金日、データ有効期限、銀行ID、銀行口座番号、クレジットカード会社ID、クレジットカード番号を含むことを特徴とするシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ICカードを利用し、クレジットサービスシステムと銀行サービスシステムを連携した決済システムに関する。

【0002】

【従来の技術】

従来、クレジットカードを利用した決済処理を行った場合、その支払いは銀行口座からの期日引落とし、もしくは小切手や現金による振込みであった。利用者はクレジットカード会社から送付される請求書に従い、期日までに代金を支払う。クレジットカード会社は、銀行や利用者からの振込みを確認した上で、支払われた金額分だけ利用可能額を引き上げるという方式を取っている。

近年、磁気カードに代わり、1枚のカードに複数のサービスが搭載可能な多機能I

Cカードが普及しつつあるが、これを用いた場合も上記方式と同様である。多機能ICカードでは、クレジットサービスを行うICカードアプリケーション（以下AP）と、銀行口座の預貯金などを行うAPが1枚のICカード上に存在可能である。

【0003】

【発明が解決しようとする課題】

上記従来技術において、クレジット決済の支払を銀行口座からの自動引落としにしている場合、利用者が銀行にクレジット利用額を入金し引落されてから、クレジットカード会社の利用可能額に反映されるまで数日かかるという問題点があった。また、通常は銀行口座からの自動引落としを支払い方式として選択する利用者が多いが、該方式だと「手元にある今、クレジット利用額を払っておきたい」「今、払った金額分をリアルタイムにクレジット利用可能額に反映させたい」という要求に対応できないという課題がある。以下では、この課題について詳細に説明する。

図1は従来のクレジットサービス決済システムの構成を表している。まず、システムの構成要素について概要を説明する。

符号101は銀行サービス提供管理システム（以下銀行システム）であり、銀行は該システムを用いて顧客情報や口座情報の管理、預貯金や引き落とし・振込みなどの銀行業務を行う。該システムには、銀行サービス提供管理サーバ（102）と銀行サービス提供管理端末（105）が存在する。銀行サービス提供管理サーバは、利用者個人口座（103）と銀行業務を行う銀行サービス提供管理処理部（104）を有する。銀行サービス提供管理端末は、銀行の各支店などに設置され、利用者が直接アクセスする、いわゆるATM端末である。

符号121はクレジットサービス提供管理システム（以下クレジットシステム）であり、クレジットカード会社は該システムを用いて顧客情報やクレジットカード情報の管理、クレジット利用時の与信チェック、決済処理などのクレジットサービス業務を行う。該システムには、クレジットサービス提供管理システム（122）とクレジットサービス加盟店端末（125）が存在する。クレジットサービス提供管理サーバは、クレジットサービス業務を行うクレジットサービス提供管理処理部（123）と、顧客情報やカード情報、顧客の与信情報などを持つデ

データベース（124）を有する。クレジットサービス加盟店端末は、クレジットカード会社と契約をした加盟店に設置され、ショッピングやキャッシングなどのクレジットサービスを利用可能な端末を有する。

銀行システムとクレジットシステム間は公衆網などのネットワークあるいは専用線によるネットワークあるいは、書面や情報記録媒体の郵送・手渡しにより情報のやり取りを実現する。また、各システムの端末／サーバ間は、公衆網もしくは専用線のネットワークにより情報のやり取りを実現する。

また、上述の銀行システム（101）とクレジットシステム（121）は、各々の処理部（104、123）に、口座管理や預貯金などの銀行業務処理機能や、クレジット決済、与信情報チェックなどのクレジットサービス処理機能を有している。これらの各処理機能は、コンピュータ・プログラムとして実現され、動作する。

次に、上記システムにおけるクレジット決済と代金支払業務の動作手順を例にとり、従来システムの課題を説明する。

クレジット決済を行った利用者（111）は、口座引落日までに銀行サービス提供管理端末（105）にアクセスし（131）、支払金額を本人の引落日指定口座（103）に入金する（132）。引落日になると銀行サービス提供管理処理部（104）はクレジットカード会社からの指定された金額を利用者口座（103）から引き出しクレジットサービス提供管理処理部（123）に振り込む（138）。クレジットサービス提供管理処理部（123）は振り込まれた金額を確認し、利用者の与信情報データベース（124）を更新する。与信情報データベースには、利用者の利用可能額と未支払金額などの情報が格納されている。利用者がクレジット加盟店端末に移動し（133）、クレジット決済を要求した際は（134）、加盟店端末はこの与信情報を確認し（135）、結果を受信し（136）、利用者に対して利用可否を提示する（137）。

ここで従来のシステムにおける第1の課題は、銀行システムからクレジットシステムへ代金が支払われてから、与信情報データベースへ反映されるまでがリアルタイムでない場合があることである。これは、振り込まれてからデータ解析処理とデータベース更新処理に時間がかかることや、銀行システムによる振込み処理

がバッチ処理であることなどに起因する。

第2の課題は、利用者が銀行システムに対して行うクレジット決済代金の入金とは、通常の預金と処理手順が変わらないため、利用者が余裕のある時に「ある時払い」を行いたい場合に、口座入金を行ってもクレジットサービスに振り込まれるのは決まった期日となるため、与信情報への反映が遅れる点である。また「口座に残っていれば使ってしまう」といった利用者の気持ちにも対応していない。利用者が「ある時払い」をしたい場合は、クレジットシステムへ振り込み処理を行う、あるいはクレジットシステムの窓口に行って直接支払うなどの通常と違った支払方法を行わなければならない。また、最近では「ある時払い」専用のカードも利用可能となっているが、これはクレジット支払方式のデフォルトが「ある時払い」であり、デフォルトの支払方法を銀行口座からの自動引落としとし、時々「ある時払い」を行いたいなどの利用者の多様な要求に柔軟に対応するのは難しい。

また「ある時払い」したい状況としては、上記のように余裕のある時に払ってしまいたいという利用者の希望だけでなく、ボーナス払いにしてある金額の引き落とし日とボーナス支給日の間にかなり開きがあるのでボーナス支給と同時に支払いたいという場合や、手元に現金があるが海外渡航するためクレジット利用可能額を引き上げておきたいといった場合がある。

以上で、従来システムにおける2つの課題についての説明を終える。

【0004】

【課題を解決するための手段】

上記課題を解決するために、本発明は利用者の入金情報を示したデータをICカード上に格納することで銀行システムとクレジットシステム間の連携可能とし、利用者が好きな時にクレジット決済の代金を銀行に入金し、その直後でも入金情報を反映したクレジット利用が可能なクレジット決済システムを提供する。

以下、詳細に説明する。

まず第1の課題である、利用者の銀行口座からの代金引落としとクレジットの与信情報への反映の間がリアルタイムでないという問題に対して本発明の実施例では、ICカード上に入金情報を示したデータを格納し、クレジット決済時はこのデー

タを確認し、与信情報の仮反映させることで解決する。本発明ではこの入金情報を示したデータをトークン（TOKEN）と呼ぶ。利用者が銀行サービスに対してクレジット決済の代金を入金した際、銀行システムはその金額、日付、有効期限などを示したトークンに自身の暗号鍵で署名し、ICカード上に格納する。ICカードには銀行サービスを行うAPが搭載されているため、ICカードとシステム間で相互認証することで該口座以外のICカードへの搭載を防ぐことが可能である。そして、利用者が直後にクレジット決済を利用する際は、直前の上金は銀行サービスからクレジットサービスへまだ振り込まれておらず与信情報データベースに反映されていないため、従来は利用可能額に直前の上金額は反映されないが、クレジットシステムにトークン検証手段を持たせることで解決する。クレジットシステムがトークンを検証し正当性を確認できた場合はトークンを信用し、記載の上金額を与信情報に仮反映させる。通常でもクレジット決済利用の際は、サーバに与信情報をオンラインで確認しているため、同時にトークンもサーバに渡すことで署名検証と与信情報への仮反映を行えばよい。また、期日には銀行システムからの振込み処理が行われているため、トークンによる仮反映の正当性を実際に確認することが可能である。

また、第2の課題である、利用者がクレジット決済の代金を払いたい時に「ある時払い」し、なおかつクレジット利用可能額へのリアルタイムな反映を行いたいという課題に対して、本発明での実施例では、銀行システム内にクレジットシステムへ振り込むべき金額を入金しておく共通の口座を設置することで解決する。本発明ではこの口座をプール口座と呼ぶ。利用者は通常は銀行の本人口座に入金し期日になると引落されるという支払方式だが、「ある時払い」をしたい場合はこのプール口座に入金する。もしくは本人口座から振替を行う。この場合も同様に銀行システムは、上金額、日付、有効期限などを示したトークンをICカード上に格納する。プール口座は利用者の本人口座ではないため、クレジット利用代金の引落日に関係なく入金すれば、それ以降の出金は不可能である。

利用者はこのトークンをクレジット決済の際に使用することで、リアルタイムな利用可能額への反映が可能となる。銀行システムは期日になったら、通常は利用者口座からの引落日するところを、プール口座からの引き落としを行いクレジット

トシステムに振込みを行う。振り込み処理はバッチ処理であることが多いが、本発明の実施例では引落とし先が利用者口座かプール口座かの違いだけであって、これまでのバッチ処理に対する修正点は少ない。

具体的に、上記2つの解決手段を用いて銀行システムとクレジットシステムが連携して行う、クレジット決済処理について説明する。まず前処理として銀行システムとクレジットシステム間でトークン用の暗号鍵を交換する。銀行システムの暗号鍵はトークンに対して署名処理を行い、銀行が生成した正当なトークンであることを示すために使用される。クレジットサービスのシステムの暗号鍵はトークンに対して暗号化処理を行い、クレジットシステム以外が復号化不可能なためトークンの秘匿性を保持するために使用される。これらの暗号鍵はオープン情報である公開鍵証明書の場合もあるし、銀行とクレジットカード会社間の契約時に専用に生成した暗号鍵である場合もあるだろう。また、暗号鍵の種類は公開鍵系暗号だけではなく、共通鍵系暗号でも可能である。以下、本特許の実施例では公開鍵系暗号鍵により説明するが、共通鍵をシステム間で交換し派生データにより派生鍵を生成させることで同様の処理が可能である。ただし、この場合は両システム間以外に対してはクローズなデータであることと、後に説明するトークンの受け渡し処理の際に派生データを付加することに注意する必要がある。

次に銀行システムによる利用者の入金処理に移る。利用者はクレジット決済の代金の入金を銀行システムに要求する。要求されたクレジットシステムが契約をしており上記処理による暗号鍵の交換を行っているかどうかを確認する。交換している場合はトークン作成が可能である。利用者の入金額をプール口座に預金し、その金額、日付、有効期限などのデータをトークンとして作成する。そして、トークンを該クレジットシステムから受領した公開鍵で暗号化し、暗号化したデータに対して自身の秘密鍵で署名をつける。この秘密鍵は上記前処理でクレジットシステムに渡した自身の公開鍵に対応するものである。このように署名・暗号化されたトークンをICカード上に格納する。ICカード上には銀行サービスを行うAPが搭載されているため、ICカード上のAPと銀行システム間で相互認証が可能である。銀行システムは、当該利用者の銀行APが搭載されたICカードであることを確認した上でトークンを搭載する。そのため、異なる利用者のICカード上にトーク

ンが搭載されず別人による不正利用を防ぐことが可能となる。またトークンはICカード上にセキュアに格納されるためコピーはできない仕組みとなっているが、もし無断コピーされた場合でも、トークン内にトークン作成日付やトークン有効期限、トークンをユニークに識別するIDなどのデータを含むことで、無断コピーによる二重使用の防止が可能となる。次の処理でクレジットシステムが使用可能とするために、トークンをICカード内で銀行APとクレジットAP間で共有する。もしくは、ICカード内の銀行APからクレジットAPへトークンを転送する。

次に銀行システムによる振込処理に移る。銀行システムは、あらかじめ設定された期日にクレジットシステムへの代金振込処理を行う。まずクレジットシステムからの引落としデータを受領する。これはどの利用者からどの金額を引落すかを記載した明細である。銀行システムは該クレジットシステムで決済を行った全利用者の支払代金をプール口座よりそれぞれ引き出す。もし利用者が「ある時払い」ではなく従来通り本人口座に入金している場合はプール口座に該当代金は入金されていないので、利用者本人口座から引き出す。本人口座残高が引落とし額に不足の場合は、引き出し不可の事実をクレジットシステムに伝える。これは従来の処理と同様である。プール口座あるいは利用者本人口座から引き出せた場合は、クレジットシステムに対して振込処理を行う。これも従来の処理と同様であり、通常は全利用者の支払代金をまとめてクレジットシステムに対してバッチ処理を行う。

次にクレジットシステムが行う処理について説明する。まず前処理として銀行システムとクレジットシステム間でトークン用の暗号鍵を交換する。銀行システムの暗号鍵はトークンに対して署名処理を行い、銀行が生成した正当なトークンであることを示すために使用される。クレジットサービスのシステムの暗号鍵はトークンに対して暗号化処理を行い、クレジットシステム以外が復号化不可能なためトークンの秘匿性を保持するために使用される。これらの暗号鍵はオープン情報である公開鍵証明書の場合もあるし、銀行とクレジットカード会社間の契約時に専用に生成した暗号鍵である場合もあるだろう。また、暗号鍵の種類は公開鍵系暗号だけではなく、共通鍵系暗号でも可能である。以下、本特許の実施例では公開鍵系暗号鍵により説明するが、共通鍵をシステム間で交換し派生データにより

派生鍵を生成させることで同様の処理が可能である。ただし、この場合は両システム間以外に対してはクローズなデータであることと、後に説明するトークンの受け渡し処理の際に派生データを付加する必要がある。

次にクレジットシステムによるクレジット決済時処理に移る。利用者はショッピングやキャッシングを行う際、クレジット決済を指定する。加盟店端末で読み取ったクレジットサービス情報を基に、クレジットシステムは与信情報をチェックする。これは現在行われている処理であり、与信情報とは、該クレジットカードあるいはクレジットAPが搭載されたICカードが紛失・盗難カードではないか、利用可能額は要求された代金に不足していないかなどの内容である。また次にICカード上のトークンを抽出し、前処理で受け取った銀行システムの公開鍵でトークンの署名を検証し正当性を確認する。確認できた場合、自身の秘密鍵でトークンを復号化する。この秘密鍵は上記前処理で銀行システムに渡した自身の公開鍵に対応するものである。ICカード上にはクレジットサービスを行うAPが搭載されているため、ICカード上のAPとクレジットシステム間で相互認証が可能である。クレジットシステムは、当該利用者のクレジットAPが搭載されたICカードであることを確認した上でトークンを抽出する。そのため、異なる利用者のICカード上のトークンを渡されるなどの不正利用を防ぐことが可能となる。またトークンはICカード上にセキュアに格納されるためコピーはできない仕組みとなっているが、もし無断コピーされた場合でも、トークン内にトークン作成日付やトークン有効期限、トークンをユニークに識別するIDなどのデータを含むことで、無断コピーによる二重使用の防止が可能となる。またトークンに含まれる利用者識別データや入金額などのデータを解析し、与信情報に仮反映させる。利用者がクレジット決済要求している金額を与信情報の利用可能額を比較し利用可否を判定し、加盟店端末に結果を提示する。以降は従来のクレジット決済処理と同様である。

次にクレジットシステムによる振込時の与信情報反映処理に移る。クレジットシステムは、銀行システムに利用者と引落し額の対応を記載した明細を渡し、あらかじめ設定された期日に銀行システムからの代金振込を受ける。クレジットシステムは振り込まれた内容により与信情報データベースを反映する。その際、トークンにより仮反映されていた情報の確認を行うことが可能であるため、不正なト

ークンによる仮反映があった場合は本処理により判明する。

以上が本発明により提供可能な処理の説明であるが、ICカード内の処理は別の方法も可能である。上記では、銀行システムがトークンを格納する際はICカード上の銀行APと相互認証し格納した。その後銀行APが同一ICカード内のクレジットAPに転送あるいは共有した上で、クレジット利用の際は、クレジットシステムがICカード上のクレジットAPと相互認証し当該トークンを抽出するといった手順であった。しかし、銀行システムがトークンを格納する際に、ICカード上のクレジットAPと相互認証し、直接クレジットAPにトークンを格納することも可能である。そのためには、銀行システムとクレジットシステム間の暗号鍵交換処理において、トークン用の鍵の他にICカード上のクレジットAPの公開鍵と、クレジットシステムに署名された銀行システムの公開鍵をクレジットシステムが銀行システムに渡すことが必要である。銀行システムは渡された署名付き自身の公開鍵をICカード上のクレジットAPに渡すことで、お互いがお互いの公開鍵を所有するため、銀行システムとICカード上のクレジットAP間での相互認証が可能となる。ICカードへのトークン格納するための当該方式も本発明の内容の一実現形式である。

また、トークンに含まれるデータとしては、利用者氏名、利用者ID、入金額、入金日、トークンID、トークン有効期限、銀行ID、銀行口座番号、クレジットカード会社ID、クレジットカード番号などである。

以上の本発明が提供するクレジット決済方法により、銀行システムとクレジットシステム間でICカード上のデータを用いた連携が可能となり、利用者が好きな時にクレジット決済の代金を銀行に入金し、その直後でも入金情報を反映したクレジット利用が可能となる。

【0005】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態を説明する。本発明に係わるシステムの基本構成は、図2に示される。図2には、符号101は銀行サービス提供管理システム（以下銀行システム）であり、銀行は該システムを用いて顧客情報や口座情報の管理、預貯金や引き落とし・振込みなどの銀行業務を行う。該システムには、銀行サービス提供管理サーバ（102）と銀行サービス提供管理端末（105）

が存在する。銀行サービス提供管理サーバは、利用者個人口座（103）と銀行業務を行う銀行サービス提供管理処理部（104）と、そして本発明の特徴であるプール口座（201）を有する。プール口座は、利用者がクレジット決済の支払代金として入金しておくために銀行が用意した一時預けのための口座であり、利用者の本人口座ではないため、クレジット利用代金の引落日に関係なく入金すれば、それ以降の出金は不可能である。銀行が引落日までの間、当該口座を用いて運用することも可能である。銀行サービス提供管理端末は、銀行の各支店などに設置され、利用者が直接アクセスする、いわゆるATM端末である。

符号121はクレジットサービス提供管理システム（以下クレジットシステム）であり、クレジットカード会社は該システムを用いて顧客情報やクレジットカード情報の管理、クレジット利用時の与信チェック、決済処理などのクレジットサービス業務を行う。該システムには、クレジットサービス提供管理システム（122）とクレジットサービス提供管理端末（125）が存在する。クレジットサービス提供管理サーバは、クレジットサービス業務を行うクレジットサービス提供管理処理部（123）と、顧客やカード、顧客の与信情報などを持つデータベース（124）を有する。クレジットサービス加盟店端末は、クレジットカード会社と契約をした加盟店に設置され、ショッピングやキャッシングなどのクレジットサービスを利用可能な端末を有する。

銀行システムとクレジットシステム間、各システムの端末／サーバ間は、基本的に公衆網や専用線などによるネットワークを通して接続され、情報のやり取りはオンライン上で電文メッセージの送受信により実現されている。しかし、運用事業者のポリシーにより書面や情報記録媒体の郵送・手渡しにより情報のやり取りを実現することも可能である。

また、本発明の実施例の構成は、銀行システム（101）とクレジットシステム（121）の各処理部（104、123）に、口座管理や預貯金などの銀行業務処理機能や、クレジット決済、与信情報チェックなどのクレジットサービス処理機能を有している。これらの各処理機能は、コンピュータ・プログラムにしたがって動作させられるものである。

次に本発明の実施例の提案方式によるクレジット決済と代金支払を行う場合の大

まかな手順を説明する。

クレジット決済処理は利用者（1 1 1）からの入金により処理は始まるが、その前処理として行うべき処理がある。それは符号 2 0 2 により示される処理であり、銀行システムとクレジットシステム間でお互いの暗号鍵を交換する処理である。これは後で説明するICカードに格納するトークン（TOKEN）に対する署名・暗号化処理のために用いる。交換する暗号鍵は、ペリサインなどの一般的な認証機関により認証された公開鍵証明書である場合もあるし、銀行とクレジットカード会社間の契約時に専用に生成した暗号鍵ペアの公開鍵である場合もある。

以上の前処理が正常に終了した場合、クレジット決済処理を行うことが可能となる。まず、利用者の入金処理に移る。クレジット決済を行った利用者（1 1 1）は、クレジット利用日から口座引落日までのいつでも好きな時に銀行サービス提供管理端末にアクセスし（2 0 3）、支払代金を銀行が設定したプール口座（2 0 1）に入金する（2 0 4）。これは現金を入金する場合もあるし、銀行の利用者本人口座（1 0 3）からの口座振替の場合もある（2 1 2）。銀行サービス提供管理処理部（1 0 4）は、入金対象のクレジットカード会社が契約済みであるかどうか、上記前処理により暗号鍵を交換しているかどうかを確認し、プール口座へのお金を行った証明としてトークンを作成し発行する（2 0 5）。トークンに含まれる事項とは例えば、利用者氏名と入金額、入金日、銀行とクレジットカード会社それぞれの事業者ID、トークンIDや有効期間などである。またこのトークンには符号 2 0 2 で受領したクレジットシステムの公開鍵による暗号化を行う。これにより、クレジットシステム以外がデータを復号化し読み取ることが不可能になるため、トークンの秘匿性を保持することが可能となる。また、暗号化したトークンに対して、銀行システムの秘密鍵による署名を付与する。この秘密鍵は符号 2 0 2 でクレジットシステムに送付した公開鍵に対応する鍵であり、クレジットシステムがトークンを受け取った際に該署名を検証することで、トークンの正当性をクレジットシステムが確認することが可能となる。このように署名・暗号化処理されたトークンは利用者が保持するICカード（1 1 0）上に格納される。ICカード上には銀行サービスを行うAPが搭載されているため、ICカード上のAPと銀行システム間で相互認証が可能である。銀行システムは、当該利用者

の銀行APが搭載されたICカードであることを確認した上でトークンを搭載する。そのため、異なる利用者のICカード上にトークンが搭載されず別人による不正利用を防ぐことが可能となる。またトークンはICカード上にセキュアに格納されるためコピーはできない仕組みとなっているが、もし無断コピーされた場合でも、トークン内にトークン作成日付やトークン有効期限、トークンをユニークに識別するIDなどのデータを含むことで、無断コピーによる二重使用の防止が可能となる。次の処理でクレジットシステムが使用可能とするため、トークンをICカード内で銀行APとクレジットAP間で共有する。もしくは、ICカード内の銀行APからクレジットAPへトークンを転送する。

クレジット利用時の処理に移る。利用者はショッピングやキャッシングを行う際、クレジット決済を指定する。加盟店端末で、クレジットサービス情報とトークンを読み取り（208）、クレジットサービス提供管理サーバに送信する（209）。クレジットサービス提供管理処理部（123）は受信したクレジットサービス情報を基に、クレジットシステムは与信情報をチェックする。これは現在行われている処理であり、与信情報とは、該クレジットカードあるいはクレジットAPが搭載されたICカードが紛失・盗難カードではないか、利用可能額は要求された代金に不足していないかなどの内容である。また次に、前処理（202）で受け取った銀行システムの公開鍵でトークンの署名を検証し正当性を確認する。確認できた場合、自身の秘密鍵でトークンを復号化する。この秘密鍵は上記前処理（202）で銀行システムに渡した自身の公開鍵に対応するものである。ICカード上にはクレジットサービスを行うAPが搭載されているため、ICカード上のAPとクレジットシステム間で相互認証が可能である。クレジットシステムは、当該利用者のクレジットAPが搭載されたICカードであることを確認した上でトークンを抽出する。そのため、異なる利用者のICカード上のトークンを渡されるなどの不正利用を防ぐことが可能となる。またトークンはICカード上にセキュアに格納されるためコピーはできない仕組みとなっているが、もし無断コピーされた場合でも、トークン内にトークン作成日付やトークン有効期限、トークンをユニークに識別するIDなどのデータを含むことで、無断コピーによる二重使用の防止が可能となる。クレジットサービス提供管理処理部（123）はトークンに含まれる利

用者識別データや入金額などのデータを解析し、与信情報データベース（124）に仮反映させる。そして、利用者がクレジット決済要求している金額を仮反映した与信情報の利用可能額と比較し利用可否を判定し、加盟店端末に結果を提示する（210）。加盟店端末はこの結果をもとにクレジット決済処理を進めるか、あるいは処理を中止する（211）。以降は従来のクレジット決済処理を同様である。

次に口座引落日における振込処理に移る。銀行システムは、クレジットシステムからの引落日データを受領する。これはどの利用者からどの金額を引落すかを記載した明細である。銀行システムは該クレジットシステムで決済を行った全利用者の支払代金をプール口座よりそれぞれ引き出し、あらかじめ設定された期日にクレジットシステムへの代金振込処理（212）を行う。もし利用者が「ある時払い」ではなく従来通り本人口座に入金している場合はプール口座に該当代金は入金されていないので、利用者本人口座から引き出す。本人口座残高が引落日額に不足の場合は、引き出し不可の事実をクレジットシステムに伝える。これは従来の処理と同様である。プール口座あるいは利用者本人口座から引き出せた場合は、クレジットシステムに対して振込処理を行う。このクレジットシステムへの振込処理（212）は従来と同様の処理であり、全利用者分をまとめてバッチ処理で振り込むことが多い。

以上が本発明に係わるシステムの基本構成と処理であるが、ICカード内の処理については2つの方法が可能であり、それに対応してシステム側の処理にも変更点が生じてくる。図14と図15を用いて詳細に説明する。図14はこれまでに説明した1番目の方式を示す図であり、銀行システムがトークンを格納する際はICカード上の銀行APと相互認証し格納した（1411）。その後銀行APが同一ICカード内のクレジットAPに転送あるいは共有した上で（1412）、クレジット利用の際は、クレジットシステムがICカード上のクレジットAPと相互認証し当該トークンを抽出する（1413）といった手順であった。しかし、銀行システムがトークンを格納する際に、ICカード上のクレジットAPと相互認証し、直接クレジットAPにトークンを格納することも可能である。図15を用いて、2番目の方法を説明する。あらかじめ銀行システムとクレジットシステム間で暗号鍵交換処理を行

うが、トークン用の鍵の他にICカード上のクレジットAPの公開鍵と、クレジットシステムに署名された銀行システムの公開鍵をクレジットシステムが銀行システムに渡しておく（1501）。銀行システムは、ICカード内の銀行APと通信するのではなく、符号1501でクレジットシステムから受け取ったICカード内クレジットAPの公開鍵を用いてクレジットAPと通信し、相互認証した上でトークンを格納する（1502）。この場合符号1503のクレジットシステムによるトークン抽出処理に関してはクレジットシステムとICカード内クレジットAPとの通信であるため変更点は生じない。

またトークンと呼ぶデータに含まれてる項目の例を示したのが図12である。利用者氏名、利用者ID、入金額、入金日、トークンID、トークン有効期限、銀行ID、銀行口座番号、クレジットカード会社ID、クレジットカード番号などを含むことで、トークンの二重使用防止や、利用者本人以外の使用防止を実現することが可能となる。

トークンの署名暗号化については図13で説明する。図12に例示されたような内容のトークンを銀行システムはまず、クレジットシステムの公開鍵で暗号化する。これにより、クレジットシステムの秘密鍵以外では復号化は不可能であり、クレジットシステム以外への秘匿性が保持される。次に、銀行システムは自身の秘密鍵で署名を付与する。この秘密鍵に対応する公開鍵は予めクレジットシステムに渡しているため、当該トークンを銀行システムが作成したことをクレジットシステムが検証することが可能となる。

以上が、システム構成を含めた全体の流れとなる。次にシステムの各構成要素について説明を行う。

図3はICカード・システムの例の概要を示す図である。ICカード110の中にはチップ302があって、リーダライタ（もしくはリーダライタを有する端末）303とデータのやりとりを行う例を示している。リーダライタの中にはコントロール・プロセッサ304やデータベースとなる磁気ディスク305などが存在する。ICカード110には、通例通り、例えば、Vcc（供給電源）、GND（グラウンド）、RST（リセット）、I/O（入出力）、及びCLK（クロック）などの諸端子が示されている。また、図中、符号306はリーダライタ303からICカード110

に対しての、例えばカードIDなどの各種問合せを示す。符号 307 は IC カードが前述の問合せに対して行った返答を示す。こうした、諸情報の伝達は通例のシステムで十分である。

【0006】

なお、IC カード内の IC チップにおいて、具体的には前述のアプリケーションはメモリ領域に搭載される。一般に、メモリとしては、RAM (Random Access Memory)、EEPROM (Electrical Erasable Programmable Read Only Memory) あるいは ROM (Read Only Memory) などが用いられる。

次に図4にこのような IC カード (110) 内に搭載されている IC 内部の基本的な領域の論理的な構成を示す。当該 IC は、通例のマイクロ・コンピュータと同様に、ハードウェア層 (403) と OS が搭載される領域、即ち OS 層 (402) とアプリケーションが搭載される領域、即ちアプリケーション層 (401) とを有する。ここで、マルチアプリケーション搭載可能とは、アプリケーション層 (401) に複数のアプリケーション (404-406) が搭載できるということである。また、アプリケーションの初期搭載とはこのアプリケーション (404-406) を IC カード発行時に既に搭載された状態で利用申請者のもとに配布することであり、ダイナミックローディング可能とはこのアプリケーション (404-406) をカード発行後に、搭載あるいは削除が可能であることを示す。OS 層 (402) は通信処理部 (407)、インタープリタ (408)、セキュリティ機構 (409) などを有し、外部端末からのコマンド受信やアプリケーションのコマンド転送などを行っている。当然、アプリケーション層 (401) と OS 層 (402) との間にはアプリケーション・インターフェイス、OS 層 (402) とハードウェア層 (403) との間にはハードウェア・インターフェイスが設置されている。

次に本発明の実施例に係わる、クレジット決済処理の具体的方法を説明する。まず図5のシーケンスを用いて利用者による入金処理とクレジット利用、代金振込処理を説明する。まず、銀行 (503) とクレジットカード会社 (504) 間でトークン用に暗号鍵を交換する (ステップ 511)。クレジットサービスを利用した利用者 (501) はその代金を期日までのいつでも好きな時に銀行に入金す

る（ステップ512）。銀行は入金したことの証明としてトークンを作成し利用者のICカード（502）に送信する（ステップ513）。次に、利用者がクレジットサービスを利用する際、ICカードからクレジットカード番号などのクレジットサービス情報とトークンを抽出し、クレジットカード会社に送信する（ステップ514）。クレジットカード会社は受信したクレジットサービス情報により、該カードが紛失・盗難カードかどうか、有効期限は過ぎてないかなどの与信情報を確認する。また受信したトークンの正当性を確認し、トークンに記載された入金額を利用可能限度額に仮反映する。仮反映した利用可能限度額を、クレジット利用を要求されている額の比較検討を行い、その結果を利用者に提示し（ステップ501）、以降は従来のクレジット利用処理を続行する。

以上で説明した本発明の実施例におけるクレジット決済方法の詳細について、銀行システムとクレジットシステムの各システムの動作フローチャート（図6～図11）を用いて説明する。これらは図5のシーケンスを詳細化したものである。

図6～図8は本発明の実施例における銀行システムの動作フローチャートである。

まず図6において銀行システムの鍵交換時処理について説明する。銀行システムはクレジットシステムと公開鍵を交換する（ステップ601）。前述したようにICカード内の処理に関連して、銀行システムがトークンをICカード内のクレジットAPに直接格納する場合は、通信を確立し相互認証するためのクレジットAP公開鍵とクレジットシステムに署名された銀行システムの公開鍵を、ステップ601でクレジットシステムから合わせて受け取っておく。

次に図7において銀行システムの利用者による入金時処理について説明する。利用者はクレジット決済の代金の入金を銀行システムに要求する（ステップ701）。銀行システムは要求されたクレジットシステムが契約をしており上記処理による暗号鍵の交換を行っているかどうかを確認する（ステップ702）。契約済でない場合は本発明に記載の方法によるクレジット利用代金の支払いはできない旨を利用者に提示し、処理を中止する（ステップ706）。契約済の場合はトークン作成が可能であるため、利用者の入金額をプール口座に預金し、その金額、日付、有効期限などのデータをトークンとして作成する（ステップ703）。

そして、トークンを該クレジットシステムから受領した公開鍵で暗号化し、暗号化したデータに対して自身の秘密鍵で署名をつける（ステップ704）。この秘密鍵は上記前処理でクレジットシステムに渡した自身の公開鍵に対応するものである。このように署名・暗号化されたトークンをICカード上に格納する（ステップ705）。ICカード上には銀行サービスを行うAPが搭載されているため、ICカード上のAPと銀行システム間で相互認証が可能である。銀行システムは、当該利用者の銀行APが搭載されたICカードであることを確認した上でトークンを搭載する。トークンは次の処理でクレジットシステムが使用可能とするため、ICカード内で銀行APとクレジットAP間で共有する。もしくは、ICカード内の銀行APからクレジットAPへトークンを転送する。また、クレジットシステムからICカード内クレジットAPの公開鍵を受け取っている場合は、ICカード内のクレジットAPと相互認証可能であり、その上でトークンを格納する。

次に図8において銀行システムの振込時処理について説明する。銀行システムは、あらかじめ設定された期日にクレジットシステムへの代金振込処理を行う。まずクレジットシステムからの引落としデータを受領する（ステップ801）。これはどの利用者からどの金額を引落とすかを記載した明細である。銀行システムは該クレジットシステムで決済を行った全利用者の支払代金をプール口座よりそれぞれ引き出す（ステップ802）。利用者が「ある時払い」ではなく従来通り本人口座に入金している場合、プール口座に該当代金は入金されていないので、利用者本人口座から引き出す。本人口座残高が引落とし額に不足の場合は、引き出し不可の事実をクレジットシステムに伝える（ステップ805）。これは従来の処理と同様である。プール口座あるいは利用者本人口座から引き出せた場合は、クレジットシステムに対して振込処理を行う（ステップ804）。これも従来の処理と同様であり、通常は全利用者の支払代金をまとめてクレジットシステムに対してバッチ処理を行う。

図9～図11は本発明の実施例におけるクレジットシステムの動作フローチャートである。

まず図9においてクレジットシステムの鍵交換時処理について説明する。クレジットシステムは銀行システムと公開鍵を交換する（ステップ901）。前述した

ようにICカード内の処理に関連して、銀行システムがトークンをICカード内のクレジットAPに直接格納する場合は、通信を確立し相互認証するためのクレジットAP公開鍵とクレジットシステムが署名した銀行システムの公開鍵を、ステップ901で銀行システムに合わせて送付する必要がある。

次に図10においてクレジットシステムの利用者によるクレジット利用時処理について説明する。利用者はショッピングやキャッシングを行う際、クレジット決済を指定し加盟店端末では受信する（ステップ1001）。加盟店端末で読み取ったクレジットサービス情報を基に、クレジットシステムは与信情報をチェックする（ステップ1002）。これは従来行われている処理であり、与信情報とは、該クレジットカードあるいはクレジットAPが搭載されたICカードが紛失・盗難カードではないか、利用可能額は要求された代金に不足していないかなどの内容である。与信情報に問題がある場合は、利用不可を利用者に提示し処理を中止する（ステップ1009）。与信情報に問題がない場合は、ICカード上のトークンを抽出し、前処理で受け取った銀行システムの公開鍵でトークンの署名を検証し正当性を確認する（ステップ1003）。正当性を確認できない場合、あるいは、トークンがICカード内に存在しない場合はトークンに関連するステップを省略しステップ1006へ続ける。ステップ1003においてトークンの正当性を確認できた場合、自身の秘密鍵でトークンを復号化する（ステップ1004）。この秘密鍵は上記前処理で銀行システムに渡した自身の公開鍵に対応するものである。次に復号化したトークンに含まれる利用者識別データや入金額などのデータを解析し、与信情報データベースに仮反映させる（ステップ1005）。利用者がクレジット決済要求している金額を与信情報データベースの利用可能額と比較する（ステップ1006）。比較結果により利用可否を判定し（ステップ1007）、利用要求額が利用可能額より大きい場合は利用不可を利用者に提示し処理を中止する（ステップ1010）。利用要求額が利用可能額の範囲内である場合は利用者に利用可能であることを提示し、クレジットサービスの利用処理を進める（ステップ1008）。以降は従来のクレジット決済処理を同様である。

次に図11においてクレジットシステムの振込時処理について説明する。クレジットシステムは、銀行システムに利用者と引落とし額の対応を記載した明細を渡し（

ステップ1101)、あらかじめ設定された期日に銀行システムからの代金振込を受ける(ステップ1102)。クレジットシステムは振り込まれた内容により与信情報データベースを反映する(ステップ1103)。その際、トークンにより仮反映されていた情報の確認を行うことが可能であるため、不正なトークンによる仮反映があった場合は本処理により判明する。

以上が本発明の実施の形態である。ICカードには接触型ICカード、非接触型ICカードなどがあるが、本発明の実施例ではこうしたICカードの構成自体によらず適用することが可能である。

【0007】

以上説明したように、本発明の実施例によれば次のようなことが可能となる。

(1) 利用者がクレジットサービスを利用し、その代金支払い方式を口座引き落としにしている場合、利用者が期日までに銀行に入金した際、その入金した情報をICカード内にセキュアに格納し、クレジット利用時にクレジットシステムにアップロードすることで、クレジット利用の利用可能額にリアルタイムに反映することが可能となる。

(2) また、利用者がクレジット利用代金を、手元にあるときに「ある時払い」を、通常利用している銀行端末を通じて行うことが可能となる。また、その際入金した情報をICカード内にセキュアに格納することで、(1)と同様にクレジット利用の利用可能額にリアルタイムに反映することが可能となる。

【0008】

【発明の効果】

利用者がクレジット利用代金を銀行口座に入金した際、入金した情報をデータ化しICカード内に格納することで、銀行サービス提供管理システムとクレジットサービス提供管理システムとの間の連携をとることが可能となる。

【0009】

また、銀行サービス提供管理システム内に、利用者がクレジットカード会社に支払う代金をまとめて入金しておく共通の口座を設けることで、利用者が手元に代金あるときや都合の良いいつでも好きなタイミングで入金する「ある時払い」を行うことが可能となる。

【図面の簡単な説明】**【図 1】**

従来のクレジット決済システム構成を示す図。

【図2】

本発明の実施形態に係るトークンを利用したクレジット利用代金支払い方法を実施するクレジット決済システム構成を示す図。

【図3】

カードシステムの概要を示す図。

【図4】

ICカードの基本構成を示す図。

【図5】

利用者の入金に応じてトークンをICカードに格納し、クレジット利用時の与信情報に反映するための本発明に係るシーケンスを示す図。

【図6】

銀行システムが、クレジットシステムと公開鍵を交換するための本発明に係るシーケンスを示す図。

【図 7】

銀行システムが、利用者からの入金要求を受け付け、トークンを作成・発行するための本発明に係るシーケンスを示す図。

【図8】

銀行システムが、期日にクレジット利用代金をクレジットシステムに振り込むための本発明に係るシーケンスを示す図。

【図 9】

クレジットシステムが、銀行システムと公開鍵を交換するための本発明に係るシーケンスを示す図。

【図 1 0】

クレジットシステムが、利用者からのクレジット利用要求を受け付け、トークンを抽出・確認し、与信情報に反映させるための本発明に係るシーケンスを示す図。

【図 1 1】

クレジットシステムが、期日に銀行からのクレジット利用代金振込みを受け付け、与信情報に反映し、トークン情報の正当性を確認するための本発明に係るシーケンスを示す図。

【図 1 2】

銀行システムが、利用者が入金したことを示すためにICカード内に格納するトークンに含まれる項目例。

【図 1 3】

トークンの署名と暗号方式例。

【図 1 4】

本発明の他の実施例を説明するための図である。

【図 1 5】

本発明の他の実施例を説明するための図である。

【符号の説明】

- 101： 銀行サービス提供管理システム
- 102： 銀行サービス提供管理サーバ
- 103： 利用者個人口座
- 104： 銀行サービス提供管理処理部
- 105： 銀行サービス提供管理端末
- 110： ICカード
- 111： 利用者
- 121： クレジットサービス提供管理システム
- 122： クレジットサービス提供管理サーバ
- 123： クレジットサービス提供管理処理部
- 124： 与信情報データベース
- 125： クレジットサービス加盟店端末
- 131： クレジット利用代金入金処理
- 132： クレジット利用代金口座入金処理
- 133： 利用者移動

- 1 3 4 : クレジット利用要求処理
- 1 3 5 : 与信情報確認処理
- 1 3 6 : 与信情報結果提示処理
- 1 3 7 : クレジット利用可否提示処理
- 1 3 8 : クレジット利用代金振込み処理
- 2 0 1 : プール口座
- 2 0 2 : 公開鍵交換処理
- 2 0 3 : クレジット利用代金入金処理
- 2 0 4 : クレジット利用代金口座入金処理
- 2 0 5 : トークン送信処理
- 2 0 6 : トークン格納処理
- 2 0 7 : 利用者移動
- 2 0 8 : クレジット利用要求処理
- 2 0 9 : クレジット利用可否確認処理
- 2 1 0 : クレジット利用可否提示処理
- 2 1 1 : クレジット利用可否提示処理
- 3 0 2 : ICチップ
- 3 0 3 : ICカード処理端末
- 3 0 4 : ICカードシステム処理部
- 3 0 5 : ICカードシステムデータベース
- 3 0 6 : ICカードコマンド要求
- 3 0 7 : ICカードコマンド応答
- 4 0 1 : アプリケーション層
- 4 0 2 : OS層
- 4 0 3 : ハードウェア層
- 4 0 4、4 0 5、4 0 6 : ICカードアプリケーション
- 4 0 7 : 通信処理部
- 4 0 8 : インタープリタ
- 4 0 9 : セキュリティ機構

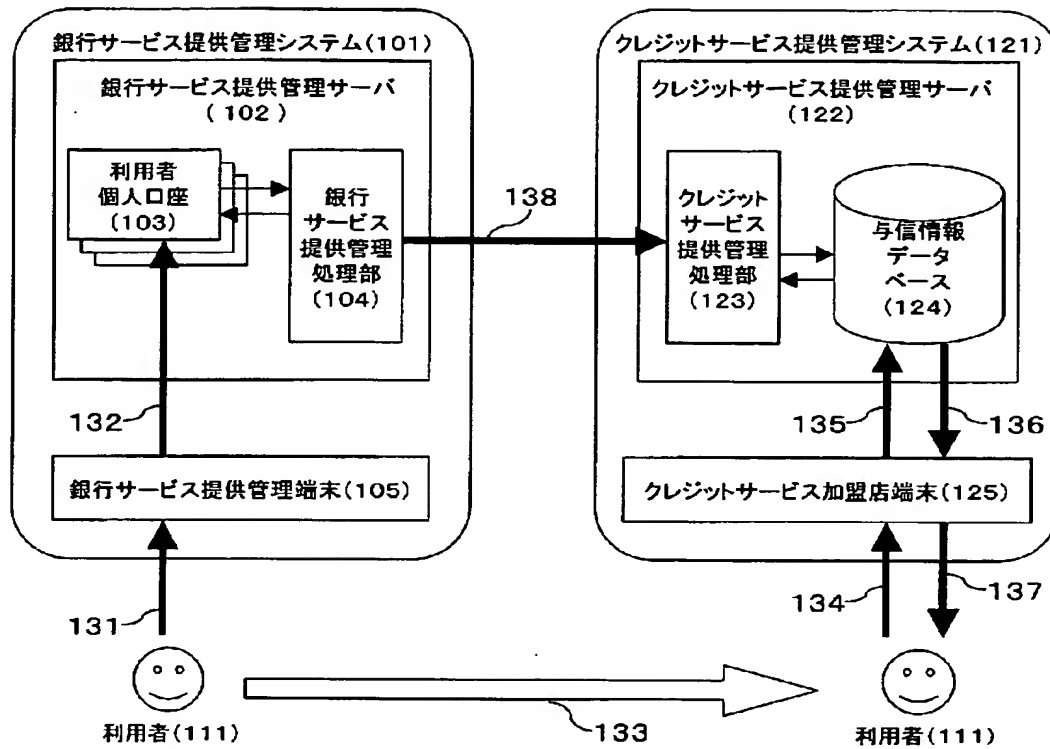
- 5 0 1 : 利用者
- 5 0 2 : ICカード
- 5 0 3 : 銀行
- 5 0 4 : クレジットカード会社
- 1 4 0 1 : ICカード内銀行サービスAP
- 1 4 0 2 : ICカード内クレジットサービスAP
- 1 4 1 1 : トークン格納処理
- 1 4 1 2 : ICカード内トークン転送処理
- 1 4 1 3 : トークン抽出処理
- 1 5 0 1 : ICカード内クレジットAP公開鍵送信処理
- 1 5 0 2 : トークン格納処理
- 1 5 0 3 : トークン抽出処理。

【書類名】

図面

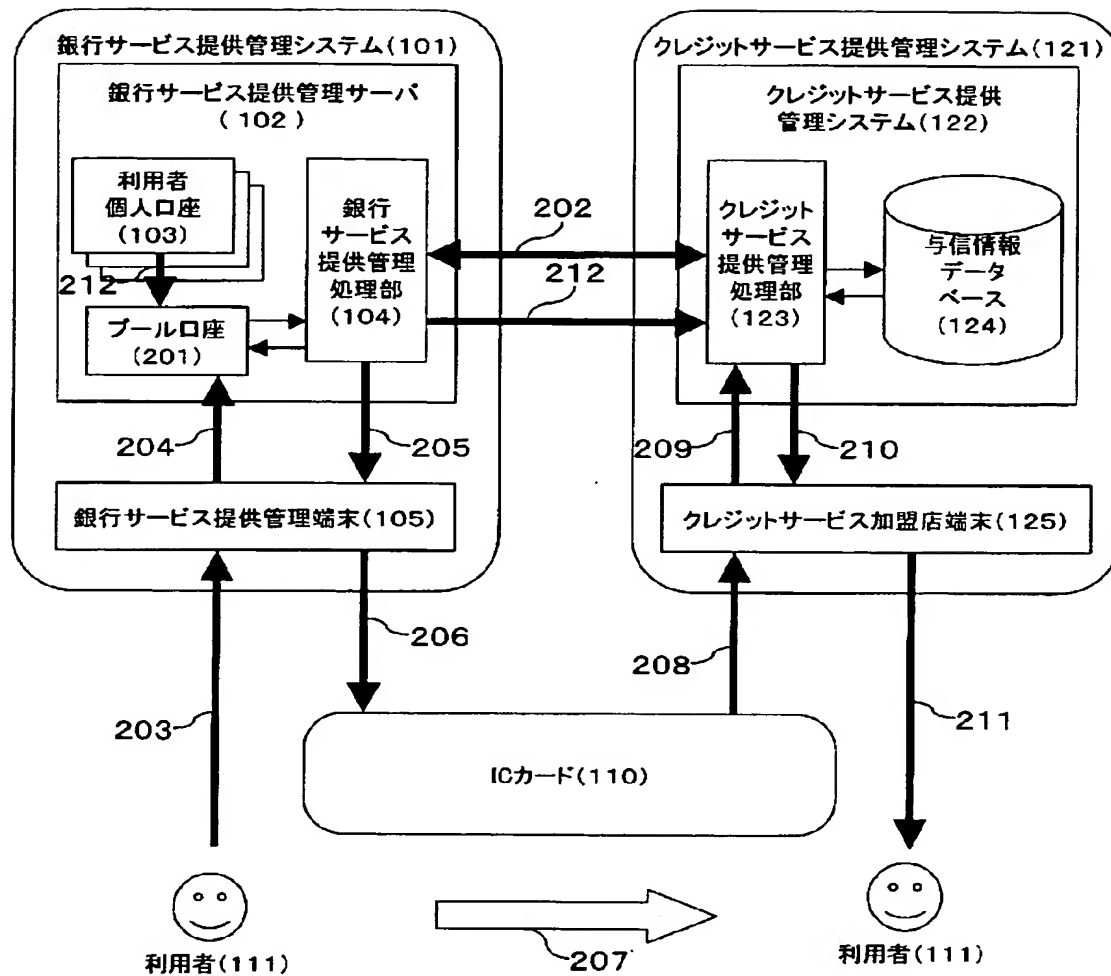
【図 1】

図1



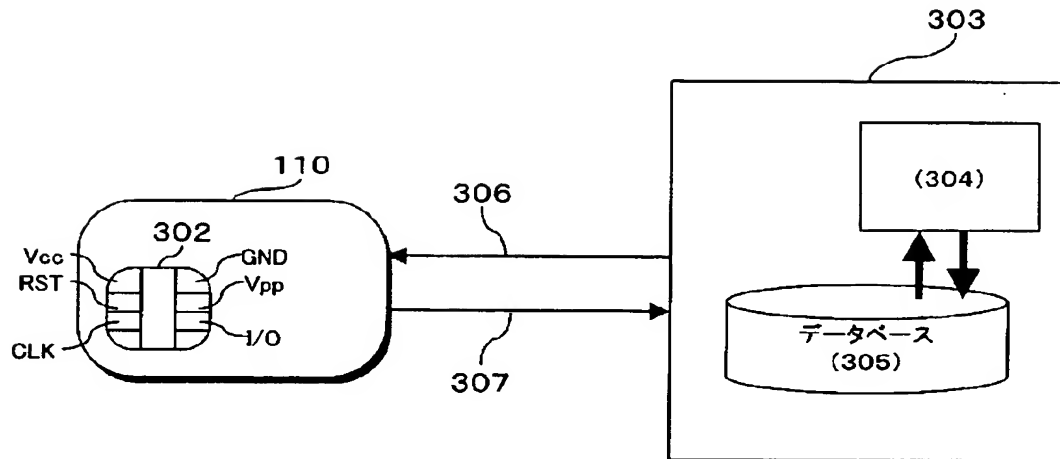
【図2】

図2



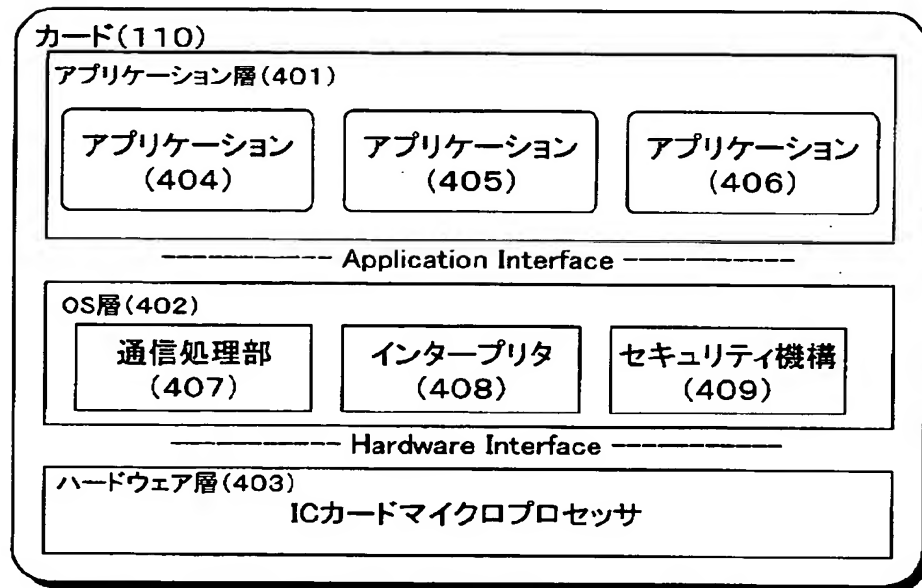
【図 3】

図3



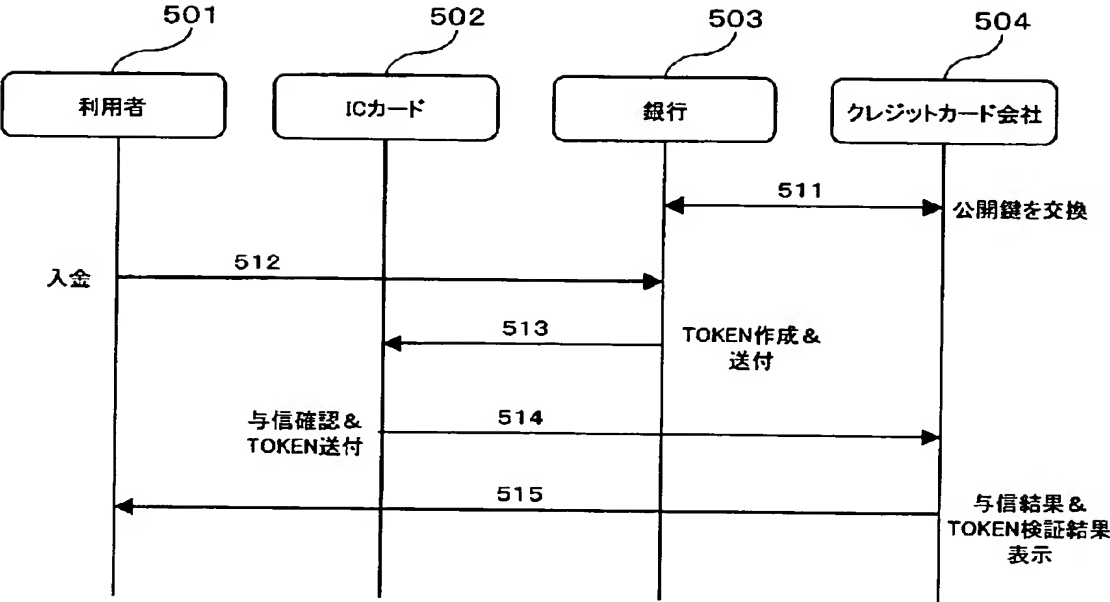
【図 4】

図4



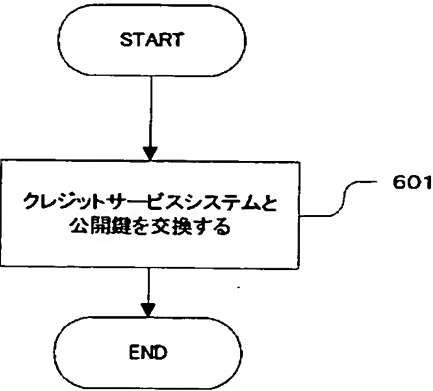
【図 5】

図5



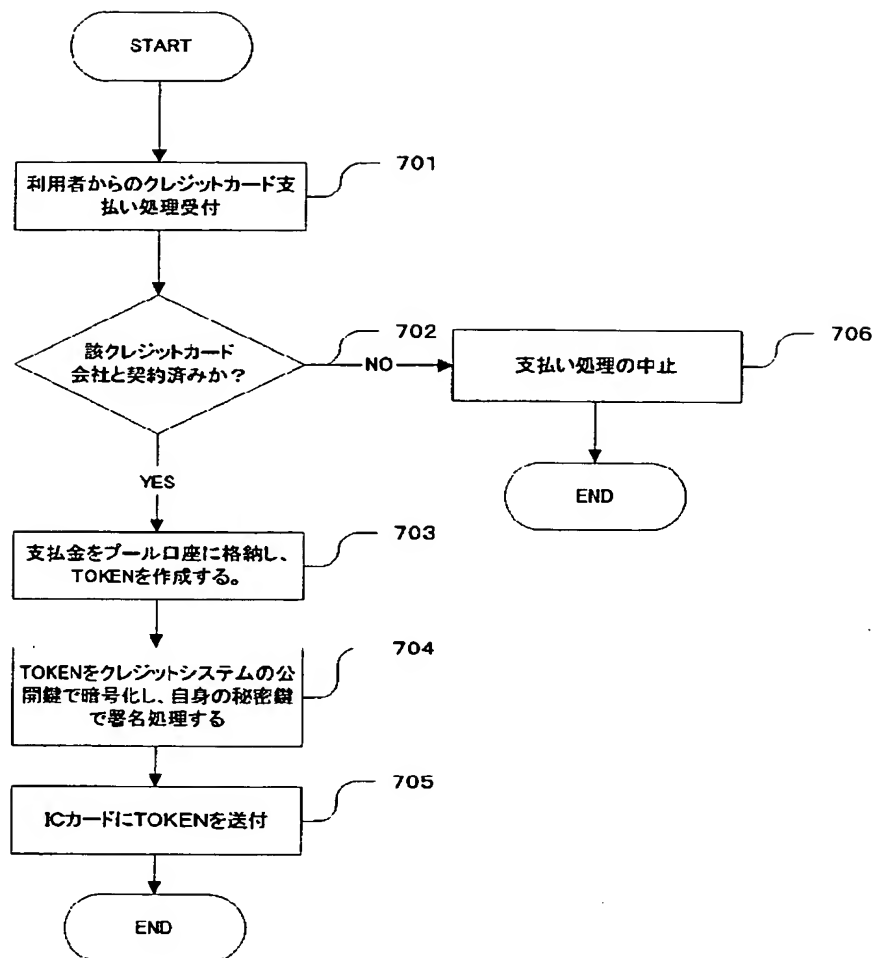
【図 6】

図6



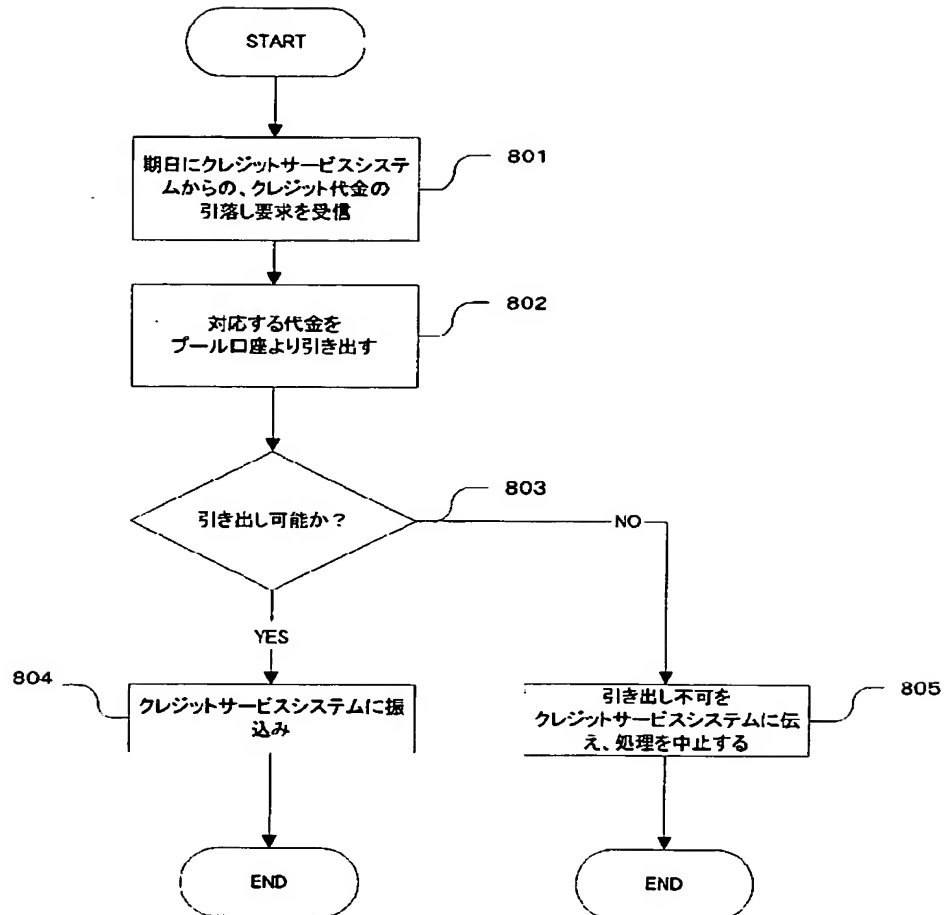
【図 7】

図7

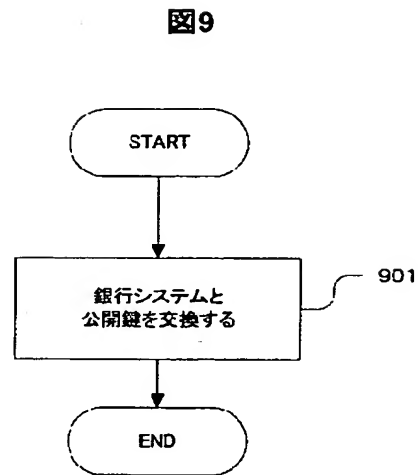


【図 8】

図8

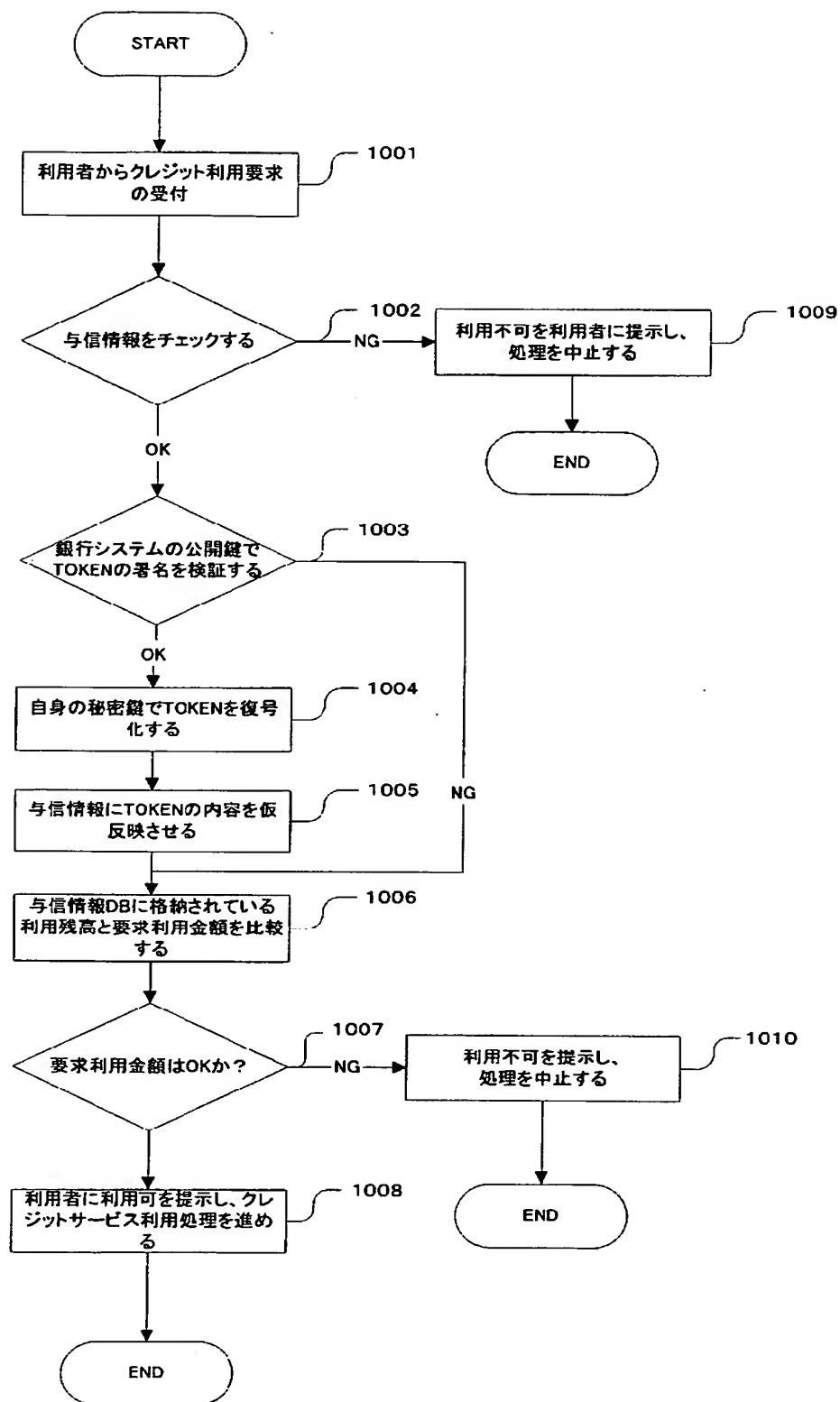


【図 9】



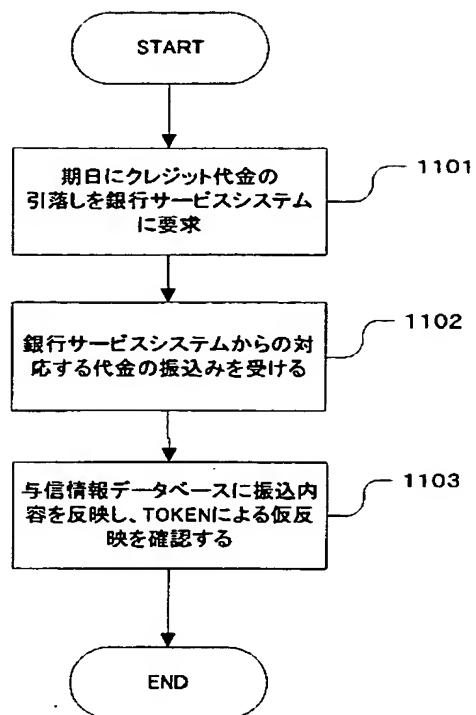
【図10】

図10



【図 11】

図11



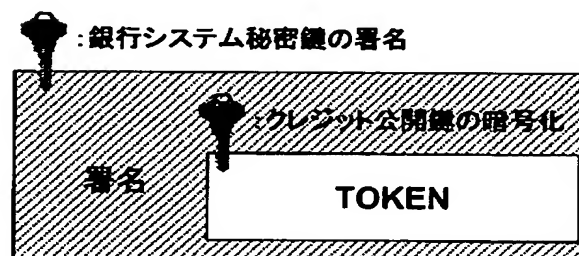
【図 12】

図12

項目	例
利用者氏名	山田太郎
利用者 ID	1000000123
入金額	¥ 40,000
入金日	2002/09/10
TOKEN ID	1234567890
TOKEN 有効期限	2002/11/15
銀行 ID	0001
銀行口座番号	999123456
クレジットカード会社 ID	1111
クレジットカード番号	1111222233334444

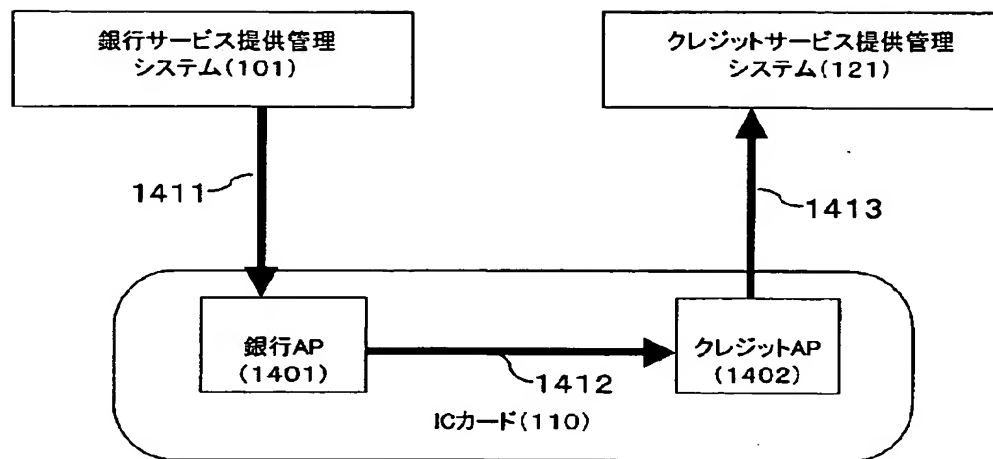
【図 13】

図13



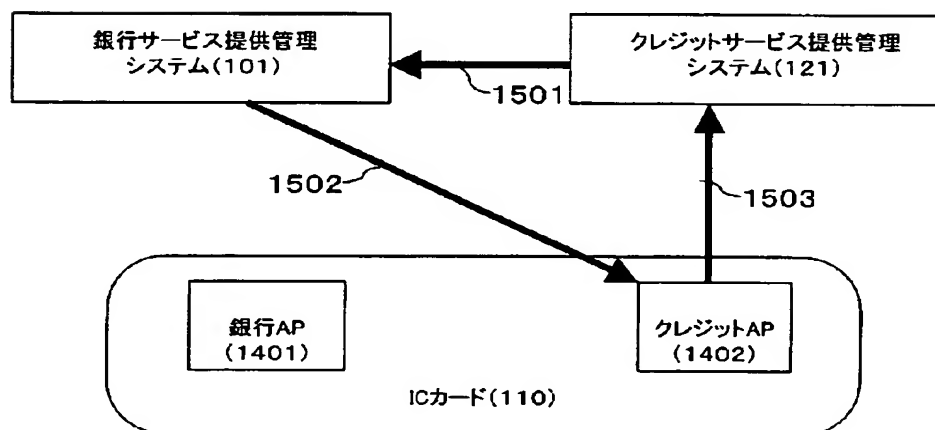
【図14】

図14



【図15】

図15



【書類名】 要約書**【要約】**

【課題】 多機能ICカードを用いたクレジット決済処理において、利用者が通常行っている銀行への入金処理を利用して、いつでも好きな時にクレジット利用代金を入金し、その後のクレジットサービス利用時においては、クレジット利用可能額へのリアルタイムな反映を可能とするための、銀行サービス提供管理システムとクレジットサービス提供管理システムを連携した、クレジット決済システムを提供する。

【解決手段】 銀行サービス提供管理システム（101）とクレジットサービス提供管理システム（121）は、必要となる公開鍵を予め交換する。銀行サービス提供管理システム（101）は利用者からのクレジット利用代金入金要求を受け、入金したことを示すデータを作成し、クレジットサービス提供管理システム（121）の公開鍵で暗号化し、自身の秘密鍵で署名付与した上で、ICカード（110）に格納する。その後、クレジットサービス提供管理システム（121）は、利用者からのクレジット利用要求を受け、入金したことを示すデータをICカードから抽出し、銀行サービス提供管理システム（101）の公開鍵により署名を検証し、自身の秘密鍵でデータを復号化した上で、与信情報データベース（124）に仮反映する。この仮反映した与信情報を用いることで、利用者は入金した金額を反映した利用可能額までのクレジット利用が可能となる。また、期日に銀行サービス提供管理システム（101）からクレジット利用代金を振り込まれたクレジットサービス提供管理システム（121）が、その内容を与信情報データベース（124）に反映することで、仮反映されていた情報の正当性を確認することが可能である。

【選択図】 図2

認定・付加情報

特許出願の番号	特願 2 0 0 2 - 3 6 9 1 7 4
受付番号	5 0 2 0 1 9 3 1 4 2 4
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 4 年 1 2 月 2 4 日

< 認定情報・付加情報 >

【提出日】	平成14年12月20日
-------	-------------

次頁無

特願 2 0 0 2 - 3 6 9 1 7 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所